PARKER DANIELS KIBORT
Andrew Parker (028314)
888 Colwell Building
123 Third Street North
Minneapolis, Minnesota 55401
parker@parkerdk.com
Telephone: (612) 355-4100
Facsimile: (612) 355-4101

OLSEN LAW, P.C.
Kurt Olsen (D.C. Bar No. 445279)*
1250 Connecticut Ave., NW, Suite 700
Washington, DC 20036
Telephone: (202) 408-7025
ko@olsenlawpc.com

Alan M. Dershowitz (MA Bar No. 121200)*
1575 Massachusetts Avenue
Cambridge, MA 02138
* Admitted *Pro Hac Vice*

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Kari Lake; Mark Finchem,

Plaintiffs,

v.

Kathleen Hobbs, as Arizona Secretary of State; Bill Gates; Clint Hickman; Jack Sellers; Thomas Galvin; and Steve Gallardo, in their capacity as members of the Maricopa County Board of Supervisors; Rex Scott; Matt Heinz; Sharon Bronson; Steve Christy; Adelita Grijalva, in their capacity as members of the Pima County Board of Supervisors,

Defendants.

No. 22-cv-00677-DMF
(Honorable John J. Tuchi)

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO STRIKE EXPERT DECLARATIONS AND TESTIMONY

Neither Fed. R. Evid. 702 nor 403 provide a basis to strike the declarations or testimony of Plaintiffs' expert witnesses Benjamin Cotton, Douglas Logan, John Mills, Shawn Smith, or Walter Daugherity. The Arizona Secretary of State's Motion to Strike Declarations & Exclude Testimony, Dkt. 74 ("Mot."), should be denied.

I.
THE EXPERTS ARE QUALIFIED UNDER RULE 702.

Defendants first say Cotton, Logan, Mills, Smith, and Daugherity are not qualified to offer expert opinions on "electronic voting systems and procedures or electronic voting system security." Mot. 3. Each expert is amply qualified to offer the testimony he provided.

For a witness to testify as an expert, Fed. R. Evid. 702 requires only that the witness have "sufficient[]" qualification by "knowledge, skill, experience, training, or education." The rule is "broadly phrased and intended to embrace more than a narrow definition of qualified expert." *Hangarter v. Provident Life & Accident Ins. Co.*, 373 F.3d 998, 1015 (9th Cir. 2004). Experience may be enough, by itself, to qualify a witness as an expert. *See id*. at 1015-16; *Thomas v. Newton Int'l Enters.*, 42 F.3d 1266, 1269 (9th Cir. 1994). The decisive question is whether the expert possesses knowledge helpful to the trier of fact: "the common sense inquiry whether the untrained layman would be qualified to determine intelligently and to the best possible degree the particular issue without enlightenment from those having a specialized understanding of the subject involved in the dispute." Notes of Advisory Comm. on Proposed Rules, Fed. R. Evid. 702 (quotation omitted). "An expert qualified by experience may testify in the form of opinion if his or her experiential knowledge will help the trier of fact to understand evidence or determine a fact in issue, as long as the testimony is based on sufficient data, is the product of reliable principles, and the expert has reliably applied the principles to the facts of the case." *Puente v. City of Phx.*, No. CV-18-02778-PHX-JJT, 2021 U.S. Dist. LEXIS 63196, at *4 (D. Ariz. Mar. 31, 2021). The rule "should be applied with a 'liberal thrust' favoring

admission." *Messick v. Novartis Pharm. Corp.*, 747 F.3d 1193, 1196 (9th Cir. 2014) (quoting *Daubert v. Merrell Dow Pharms..*, 509 U.S. 579, 588 (1993)).

. "Disputes as to the credentials, methodology, or basis for an expert's opinion generally 'go to the weight, not the admissibility, of his testimony.'" *ReBath LLC v. HD Sols. LLC*, No. CV-19-04873-PHX-JJT, 2022 U.S. Dist. LEXIS 119997, at *8 (D. Ariz. July 7, 2022) (quoting *Kennedy v. Collagen Corp.*, 161 F.3d 1226, 1231 (9th Cir. 1998)).

Each of the experts proffered by Plaintiffs has extensive knowledge that will help the trier of fact understand evidence or determine facts in issue.

Cotton. Cotton's experience providing cybersecurity analysis, forensics, and incident response services to private sector and federal government clients for many years plainly qualifies him to offer expert testimony in the field of computer system security, vulnerabilities, risks, and threats. *See* Decl. of Benjamin R. Cotton ¶¶ 3-8 (Dkt. No. 35). He performs computer forensics, e-discovery, and cybersecurity incident response services for public and private sector clients. Tr. of Hearing at 15:18-16:5; 17:15-22 (July 21, 2022) ("Hearing Tr."). If that were not enough, he testified that he created the cybersecurity tool that discovered the Chinese breach of the federal government's Office of Personnel Management computer network – which government cybersecurity measures had not prevented or identified. Hearing Tr. 16:6-17:1. Cotton has expert knowledge about cybersecurity principles, practices, and threats, and the application of cybersecurity standards, that the untrained lay person does not have. This knowledge is helpful to the finder of fact in assessing the technical concepts presented by this action. The suggestion that Cotton is not qualified to offer expert testimony on cybersecurity borders on frivolous.

It may be that Defendants' motion is premised on a purported distinction between expertise in *computer* systems and computer *voting* systems. However, Cotton and Logan testified that computer voting systems, with respect to cybersecurity, are not different from other computer networks. Hearing Tr. 53:22-54:4; 59:19-60:2 (cybersecurity

analysis of computer systems and cybersecurity analysis of voting election machine computer systems is "exactly the same" and "like any other computer system with a complex application on it"). A computer voting system is merely a computer or computer network with an election software package. Cotton is qualified to offer expert testimony on the cybersecurity of computer voting systems.

Defendants argue that there is a "need for specificity in the field of election law." Mot. at 3. Plaintiffs' experts, however, did not provide expert testimony concerning "the field of election law." Their testimony concerns the technical and practical aspects of computer systems and cybersecurity, which are applicable to election computers just as they are to any computers. The cases cited by Defendants on election law testimony are not comparable to the situation here.

Moreover, Cotton provided fact testimony about his personal examinations of the relevant and related computer systems. He is qualified to testify as fact witnesses and provide expert opinions, much like a treating physician.

Logan. Logan has roughly two decades of information technology experience, and more than ten of those years have been "specifically focused in Cyber Security in the area of Application Security." Decl. of Douglas Logan ¶ 3 (Dkt. No. 39). He has held multiple cybersecurity related certifications, developed cybersecurity programs, and led cybersecurity services for the federal government, JPMorgan Chase, and Bank of America related to hacking, malicious code detection, code review, and threat modeling. *Id*. ¶¶ 4-5. He has personally overseen or conducted more than 2,000 software application vulnerability assessments, with clients in the federal government and major industries. *Id*. ¶ 8. He has conducted penetration testing, malicious code detection, and threat modeling. Hearing Tr. 58:7-14. He also served as lead cybersecurity advisor for a federal agency for two years. *Id*. 59:8-18. Logan is qualified to offer expert testimony concerning the cyber security and cyber vulnerabilities of Arizona's election computer system.

Like Cotton, Logan provided fact testimony about his personal examinations of

the relevant and related systems. He, too, is qualified to testify as fact witnesses and provide expert opinions.

Mills. Mills is the former Director of Cybersecurity Policy, Strategy, and International Affairs at the Office of the Secretary of Defense. Decl. of John R. Mills ¶ 2 (Dkt. No. 40). He has many years of experience dating back to leadership roles at a time when cybersecurity first emerged as a critical security function. He has taught graduate level cybersecurity law and policy at the University of Maryland for nine years. *Id*. He is personally familiar with government capabilities to manipulate critical infrastructure, including election systems, worldwide. *Id*. ¶ 15. He has performed hundreds of reviews of cybersecurity breaches of systems to provide findings and recommendations for remediation. Hearing Tr. 88:6-13. Mills is qualified to offer expert testimony concerning the risks of cybersecurity breaches, the means of cybersecurity breaches, the types of cybersecurity breaches, and what is necessary to prevent cybersecurity breaches – even in circumstances of the most security-hardened computer systems.

Smith. Smith has more than twenty-five years of experience operating, specifying requirement for, planning procurement, testing, and commanding complex, computer-based military weapon systems. Decl. of Shawn A. Smith ¶ 3 (Dkt. No. 41). He served for four years as the Senior Military Evaluator for Space and Intelligence, Surveillance, and Reconnaissance systems in the office of the Director, Operational Test & Evaluation, under the Office of the Secretary of Defense. *Id*. ¶ 5. He has advised U.S. federal agencies concerning opportunities and technical approaches for supply chain compromise. *Id*. ¶ 4. After retiring from the U.S. military, he continued to consult with the federal government concerning cyber threat conduct against national security targets, and his conclusions were provided to senior military officials, the Secretary of Defense, and the President. *Id*. ¶ 6. Smith is qualified to offer expert testimony concerning supply chain compromise risks and effects, and the efficacy of attempts to prevent them, including his knowledge of the breach of the CISA network which persisted for ten months before it was

discovered.

Daugherity. Daugherity taught computer science and engineering at Texas A&M for 32 years, and elsewhere for five years prior to that. Decl. of Walter C. Daugherity ¶ 2 (Dkt. No. 38). He has served as a computer consultant to major firms and government agencies. *Id*. ¶ 4. He holds advanced degrees in mathematics and mathematical education from Harvard. *Id*. Ex. A. Daugherity is qualified to offer expert testimony on the mathematical and computer significance of voting data reported through Arizona's election computer systems.

II.
DEFENDANTS' MISCELLANEOUS ASSERTIONS PROVIDE NO BASIS FOR EXCLUSION.

Defendants advance various assertions that purportedly require exclusion of Plaintiffs' experts. Mot. at 4-5. These assertions are not supported by law or facts.

Arizona Specificity. Defendants attack Mills's and Smith's declarations as disconnected from "Arizona's voting systems and procedures." *Id*. at 4. This argument relies upon an invalid legal premise, and is factually incorrect.

Defendants' invalid legal premise is the assumption that an expert's testimony may only be admitted if the expert possesses expertise concerning the locality of the litigation. This is simply wrong. An expert may provide testimony about technical principles without connecting them to the specific facts of the case at hand, "leaving the trier of fact to apply them to the facts." Notes of Advisory Comm. on Proposed Rules, Fed. R. Evid. 702. Mills and Smith provide specialized knowledge concerning the existence, extent, and characteristics of cybersecurity threats in the world today. The information they provide is not known to the average lay person, and the threats they describe relate to all "critical infrastructure" computer systems in the United States, including Arizona's election computer systems. Experts may rely on their "specialized knowledge and experience" as "the requisite 'facts or data' on which they render an opinion." *Elosu v. Middlefork Ranch Inc.*, 26 F.4th 1017, 1024 (9th Cir. 2022); *see Meador v. Aramark*

Sports & Entm't Servs. LLC, No. CV-19-08345-PCT-JJT, 2021 U.S. Dist. LEXIS 78909, at *15-16 (D. Ariz. Apr. 23, 2021) ("Even if true, this is not disqualifying. Mr. Derie is not a scientific expert; rather, his testimony is based on knowledge and experience."). *Even if* Mills and Smith made no attempt to connect their knowledge of cybersecurity threats and principles to the facts of this case, their knowledge is relevant and assists the finder of fact in understanding what kinds of breaches vulnerable computer systems can suffer. But Defendants are factually incorrect as well as legally incorrect. Smith and Mills do apply their experience to the specific facts of Arizona's election systems – also a permissible function for an expert. "It will continue to be permissible for the experts to take the further step of suggesting the inference which should be drawn from applying the specialized knowledge to the facts." Notes of Advisory Comm. on Proposed Rules, Fed. R. Evid. 702.

Defendants' own evidentiary presentation implicitly admits that an expert in cybersecurity may apply his or her knowledge to multiple fields including election systems. Defendants' witness Ryan Macias, who himself cannot be considered a cybersecurity technical expert, testified that he was a "consultant" in "election technology and election security" as well as "other areas of critical infrastructure, including health care, ICT . . . and communications technology." Hearing Tr. 129:9-20; 132:6-7 ("Secretary of Department of Homeland Security J. Johnson named elections critical infrastructure"). Macias's testimony, in addition to Cotton's and Logan's testimony quoted above, acknowledges the reality that Mills and Smith describe – the same cybersecurity threats and principles apply across industries.

Past Expert Witness Testimony. Defendants assert that Plaintiffs' experts have not testified as expert witnesses before. Mot. at 4-5. Cotton testified that he has. Hearing Tr. 17:2-14. In any event, Rule 702 imposes no requirement of prior testimonial experience.

Statement of Experience. Defendants assert that Smith, Mills, and Cotton have not "provided a current curriculum vitae." Mot. at 4, 5. Rule 702 imposes no C.V.

requirement. In any event, Smith's and Mills' testimony and declarations provide ample information about their qualifications and experience, and Cotton's C.V. was provided by Plaintiffs as Exhibit T at the July 21, 2022, hearing.

Daugherity. Defendants attack Daugherity for a purported lack of "connection or experience with Arizona." Mot. 6. Rule 702 imposes no requirement that an expert live in or travel to the state that his testimony concerns. Defendants attack Daugherity's training and knowledge about tabulation or recording procedures, and his methodology. Mot. at 4-5. Daugherity's declaration states clearly the data he relied upon, the analysis he performed of it, and the reasons for his conclusions. A methodology is not excludable merely because it is new or because it is a new application of the expert's methods; "Experts working in specialized, scientific, and uncertain fields regularly 'extrapolate from existing data' and generate novel hypotheses about complex issues." *Elosu*, 26 F.4th at 1026 (quoting *GE v. Joiner,* 522 U.S. 136, 146 (1997)). Defendants do not explain – and cannot explain – why it would be impossible to apply Daugherity's mathematical and computer science background in the context of Arizona election data. Their generalized rhetorical criticisms of Daugherity's analysis, Mot. at 6-7, do not identify any actual problem with it. They were entitled to provide expert testimony – or even a reasoned explanation, in their Motion – to rebut, dispute, or call into question Daugherity's declaration, which was filed and served on June 8, 2022, six weeks prior to the hearing. Dkt. 38. They did not do so. Their non-specific disagreement with his conclusions provides no basis for exclusion or limitation of his testimony under Rule 702.

III.
THE EXPERTS' OPINIONS ARE SUPPORTED.

Defendants next assert Plaintiffs' experts' opinions are "ipse dixit." Mot. 5-6. This argument relies upon mischaracterizing the testimony in order to impose a non-applicable standard. The *Daubert* factors cited by Defendants, Mot. 5-6, "may not apply to testimony that depends on knowledge and experience of the expert, rather than a particular

methodology." *Puente*, 2021 U.S. Dist. LEXIS 63196, at *4 (citing *U.S. v. Hankey*, 203 F.3d 1160, 1169 (9th Cir. 2000)). Without regard to considerations of peer review, testing of methodology, error rate, and general acceptance, "[a]n expert qualified by experience may testify in the form of opinion if his or her experiential knowledge will help the trier of fact to understand evidence or determine a fact in issue, as long as the testimony is based on sufficient data, is the product of reliable principles, and the expert has reliably applied the principles to the facts of the case." *Puente*, 2021 U.S. Dist. LEXIS 63196, at *4 (citing Fed. R. Evid. 702; *Daubert*, 509 U.S. at 579).

Four of Plaintiffs' five experts possess deep experience and knowledge about cybersecurity, either from the perspective of specifically analyzing particular systems and software (including the specific system at issue here) for vulnerability and existing breaches, or from the perspective of studying and working to prevent systemic cybersecurity breaches. The fifth expert, Daugherity, stated a method of statistical analysis derived from his mathematical background and his experience with PID controllers. In all cases the experts have offered testimony drawn from applying their deep experience to the sufficient data provided by the facts of the case, and their declarations and testimony explain why they have reached the conclusions they state. Defendants' attempt to impose requirements of peer review, testing, established error rate, and general acceptance is improper, and Defendants ignore the explanations given by Plaintiffs' experts to support their testimony.

IV.
THE EXPERTS' TESTIMONY IS HELPFUL.

Defendants lastly argue that the testimony of Plaintiffs' experts will not "logically advance a material aspect" of a party's case and is not "relevant" under Rule 403. Mot. 7-8. This argument erroneously assumes that *only* a past incident of *actual* cybersecurity breach of a *voting system* within *Arizona* has any relevance to Plaintiffs' claims. *See id*.

Defendants' assumption asserts an absurdly narrow conception of evidentiary

relevance. Evidence that Arizona's vulnerable voting computers leave an open door for unauthorized manipulation supports Plaintiffs' claims that Defendants have not established a vote counting procedure calculated to yield an accurate result (against Defendants' assertions that their system is reliable and accurate). Evidence that cybersecurity breaches of computer networks generally are common and dangerous supports Plaintiffs' claims that malicious actors are likely to exploit the identified security failures in Defendants' computer systems (against Defendants' minimization of that likelihood). This is particularly the case when dealing with a system which has been designated a part of the U.S. critical infrastructure. Evidence that voting and voting-related systems in Arizona and elsewhere actually have been breached supports Plaintiffs' claims that malicious actors seek to engage in unauthorized manipulation of U.S. elections (against Defendants' dismissal of that threat).

Defendants in essence argue that no lawsuit can be brought to challenge Arizona's election computers until *after* an election *is actually manipulated* in Arizona. That is not the standard for litigation to prevent constitutional violations.[1] The same logic would dictate that if Arizona announced it would conduct elections by voters writing their votes as tally marks on an unmonitored chalkboard in the center of town, relying on the honor system, no evidence of the security weaknesses of this method would be relevant unless the evidence came from actual elections conducted in Arizona using the same method.

Evidentiary relevance is not so narrowly circumscribed. Evidence is relevant if "it has any tendency to make a fact more or less probable than it would be without the evidence" and "the fact is of consequence in determining the action." Fed. R. Evid. 401.

---

[1] Moreover, because Defendants only hand-count the paper ballots in 2% of precincts in an election, it is likely that any unauthorized computer manipulation of election results will go undetected. Defendants thus assert they are immune to evidence of the ease with which their computer election results can be manipulated, until such time as an unauthorized manipulation for which they are not looking is found.

"To warrant the use of expert testimony, two elements are required. First, the subject of the inference must be so distinctly related to some science, profession, business or occupation as to be beyond the knowledge of the average layman, and second, the witness must have such knowledge or experience in that field or calling as to make it appear that his opinion or inference will probably aid the trier of fact in his search for truth." *Shad v. Dean Witter Reynolds, Inc.*, 799 F.2d 525, 529 (9th Cir. 1986) (quoting *Fineberg v. United States*, 393 F.2d 417, 420 (9th Cir. 1968)). Both of those elements are present here, for each of Plaintiffs' experts. Their testimony shows that Arizona's election computer systems are vulnerable to manipulation in many ways:

- Antivirus updates are not performed, leaving the system vulnerable to vast amounts of new malicious code created on a daily basis. Cotton Decl. ¶ 18(a) (Dkt. No. 35); Hearing Tr. 22:9-23 (Cotton); Hearing Tr. 179:23-180:19 (Jarrett).
- Software patches are not performed, leaving the system open to exploitation of vulnerabilities regularly identified and publicized by Microsoft. Cotton Decl. ¶ 18(b); Hearing Tr. 23:1-24:2 (Cotton).
- Passwords are shared between users and the administrator password for the system is not changed, permitting multiple people the ability to anonymously make modifications to the system. Cotton Decl. ¶ 18(c); Hearing Tr. 24:3-6, 15-22 (Cotton); Second Cotton Decl. ¶ 2 (Dkt. No. 89).
- The system lacks necessary activity and network monitoring functions to detect the presence of unauthorized activity. Cotton Decl. ¶ 18(d); Hearing Tr. 54:20-55:9 (Cotton).
- The system lacks adequate log management practices to record access to and activities performed within it. Cotton Decl. ¶ 18(e) & 18(e)(iv); Hearing Tr. 25:2-26:14; 53:3-20 (Cotton).
- The system logs that do exist are exposed to modification by users, meaning

an unauthorized user could make changes to the system and then delete any log entries that recorded this activity. Cotton Decl. ¶ 18(e)(i).

- The system logs that do exist are subject to overwriting after a fixed limit of events is recorded, meaning important data can be lost simply through the passage of time. Cotton Decl. ¶ 18(e)(iv); Hearing Tr. 25:2-26:14; 53:3-20 (Cotton).
- Computers within the system contained wireless modems and wifi cards that could be used to connect them to unauthorized networks and expose them to unauthorized changes. Cotton Decl. ¶ 18(f); Second Cotton Decl. ¶ 1; Hearing Tr. 27:14-28:17 (Cotton).
- The EMS server and computers connected to it had unblocked ports that provide a means of accessing them. Second Cotton Decl. ¶ 2.
- The system lacked any mechanism for blocking malicious activity or programs, except for the outdated antivirus program. Cotton Decl. ¶ 18(g).
- Computer systems can be compromised by malware implanted in their hardware components at the time of manufacture overseas, and it cannot be determined for certain whether such a supply chain compromise has already affected Arizona's election computers. Smith Decl. ¶¶ 8, 12-15, 59, 78-80 (Dkt. No. 41); Hearing Tr. 61:21-62:10 & 63:22-64:3 (Logan); 93:12-25 (Mills); *cf.* Hearing Tr. 136:2-4 (Macias).
- Foreign attempts to interfere in U.S. election-related computers have been detected on multiple occasions, and major foreign hacks of theoretically secure U.S. government computer networks have occurred on multiple occasions. Smith Decl. ¶ 20; Parker Decl. ¶ 11 & Ex. J (Dkt. No. 42).
- Remote attacks against computer networks have become an ordinary aspect of international intelligence efforts, and foreign nations have established organized groups of specialists who systematically plan and conduct remote

attacks against computer networks. Mills Decl. ¶ 4-6, 11, 15, 36-37, 42-44 (Dkt. No. 40); Smith Decl. ¶ 29.

- U.S. election computer systems have repeatedly been hacked in demonstrations by university professors and hacking convention attendees, and experts have said that election computers have *always* been found vulnerable to hacking, when they have been examined. Logan Decl. ¶¶ 43-47; Parker Decl. ¶ 8 & Ex. G at 35; Parker Decl. ¶ 9 & Ex. H at 72. 76.

This information provided by Plaintiffs' experts about cybersecurity breaches, threats, defenses, and practices is relevant information that an average lay person does not know – and which would be difficult or impossible to enter into evidence through any means *other than* expert testimony.

V.
DEFENDANTS FAIL TO PROVIDE ANY COMPETENT CHALLENGE TO PLAINTIFFS' EXPERTS.

Defendants broadly assert that the testimony of Plaintiffs' experts is "unreliable," "unscientific," "based on a literature review," "speculative," and not "sound or reliable." Mot. 1, 3, 6, 7, 8. This is inaccurate and ignores the record. Moreover, Defendants fail to offer anything more than attorney argument to support these (incorrect) characterizations. They provide the Court with *no* testimony from any individual knowledgeable about or experienced in personally evaluating the cybersecurity of any computer system. Nor do they show how any particular aspect of any expert's opinion is defective in any of these ways. Accordingly, Defendant's assertions about the reliability of Plaintiffs' expert testimony are meaningless.

The only evidence Defendants provide is (1) declarations from three county elections directors, Constance Hargrove (Dkt. No. 59-1), Lisa Marra (Dkt. No. 59-2), and Rayleen Richards (Dkt. No. 59-3), none of whom claim any technical computer expertise

and all of whom direct their statements toward the logistics of hand counting ballots;[2] (2) a declaration (Dkt. No. 57-1) and testimony from Scott Jarrett, a county elections department co-director who does not claim any technical computer expertise, and who testified about the Maricopa County election computer system's equipment, Maricopa County election procedures, and the logistics of hand counting ballots; (3) testimony and a C.V. (Defs.' Ex. 4) from Ryan Macias; and (4) a list of election equipment (Defs.' Ex. 5) and a Maricopa 2022 Elections Plan (Defs.' Ex. 6).

Thus Defendants' sole "evidence" concerning cybersecurity issues is the conclusory opinion of Ryan Macias, an individual who does not claim any personal technical computer expertise, and who has no education or experience concerning cybersecurity analysis of computer systems. *See* Defs.' Ex. 4. Mr. Macias has served as a "consultant" and administrative agency employee. Hearing Tr. 129:11, 134:10-136:8. While he claims "familiarity" with the security and reliability of Arizona's election systems, *id*. 134:7-9, he does not claim to have performed any cybersecurity analysis of such a system himself. When asked, "What do you do?" he responded that he works on "building resiliency in the elections process" and "provide[s] best practices." *Id*. 129:21-130:1, 130:6-7. Mr. Macias's testimony showed he has experience in going to meetings, giving speeches, supervising others, and doing unspecified "work[]" "with" various entities, *see id.* 129:9-131:7 & 159:8-13; 136:11-23; 134:25-135:3; 130:15-131:7, but not any experience wrestling with real computer systems and real cybersecurity incidents and threats.

The contrast between Mr. Macias and Plaintiffs' experts is illustrative. Macias

---

[2] Plaintiffs showed at the July 21, 2022 hearing that Maricopa County has 225 sites established for the voting during the November 2022 general election, and that if tables are set up at each of these sites, 2,000 ballots could be counted in a reasonable time at each individual table. If two million ballots were cast in the election in Maricopa County (which would be historically unprecedented in an off-year election, *see* Pls.' Ex. Q) five counting tables at each of 225 sites would be sufficient to count the ballots. *See* Hearing Tr. 204:5-205:24.

provides the Court with vague, conclusory generalizations about "working with" and "advising" on elections issues, but not personally analyzing any computer system. Macias either lacks any technical basis for his opinions or else relies on the technical expertise of other, unidentified people. Either way, his testimony affirming the security and reliability of Arizona's election systems provides no technical assistance to the finder of fact – it is bare opinion unconnected to any personal knowledge of Macias. In contrast, Plaintiffs' experts routinely and regularly handle real-world computer systems to address the cybersecurity needs of real-world, paying clients. They have personal technical experience to offer the finder of fact, not merely the say-so that someone else somewhere thinks something about an election system. Plaintiffs' experts describe their analysis of Arizona's election computer systems and the resulting conclusions.

Defendants offer no technical or evidentiary support for their assertions that Plaintiffs' expert testimony is "unreliable," "unscientific," "based on a literature review," "speculative," or not "sound or reliable." Their argumentative opinions provide no basis to exclude Plaintiffs' witnesses.

VI.
CONCLUSION

"Rule 702 does not license a court to engage in freeform factfinding, to select between competing versions of the evidence, or to determine the veracity of the expert's conclusions at the admissibility stage. This is consistent with the basic function of expert testimony: to help the trier of fact understand highly specialized issues that are not within common experience." *Elosu*, 26 F.4th at 1026. "A factual dispute is best settled by a battle of the experts before the fact finder, not by judicial fiat. Where two credible experts disagree, it is the job of the fact finder, not the trial court, to determine which source is more credible and reliable." *City of Pomona v. SQM N. Am. Corp.*, 750 F.3d 1036, 1049 (9th Cir. 2014). While Plaintiffs' motion seeking preliminary injunctive relief places the Court in the position of the finder of fact, the Court's analysis of Plaintiffs' expert

evidence must be done on a substantive basis; the evidence is not excludable under evidentiary rules.

Defendants' Motion at most presents arguments for the finder of fact to weigh when assessing the credibility of Plaintiffs' expert evidence. The Motion does not provide any basis for excluding the testimony *ab initio* and should be denied.

DATED: July 27, 2022

PARKER DANIELS KIBORT LLC

By */s/ Andrew D. Parker*
Andrew D. Parker (AZ Bar No. 028314)
888 Colwell Building
123 N. Third Street
Minneapolis, MN 55401
Telephone: (612) 355-4100
Facsimile: (612) 355-4101
parker@parkerdk.com

OLSEN LAW, P.C.

By */s/ Kurt Olsen*
Kurt Olsen (D.C. Bar No. 445279)*
1250 Connecticut Ave., NW, Suite 700
Washington, DC 20036
Telephone: (202) 408-7025
ko@olsenlawpc.com

By */s/ Alan M. Dershowitz*
Alan M. Dershowitz (MA Bar No. 121200)*
1575 Massachusetts Avenue
Cambridge, MA 02138
* Admitted *Pro Hac Vice*

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on July 27, 2022, I electronically transmitted the foregoing document to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the CM/ECF registrants on record.

/s/ Andrew D. Parker